WE CLAIM AS OUR INVENTION AND DESIRE TO SECURE PROTECTION FOR:

1. A method of protecting a data signal comprising the steps of:

applying a data reduction technique to reduce the data signal into a reduced data signal;

subtracting said reduced data signal from the data signal to produce a remainder signal;

embedding a first watermark into said reduced data signal to produce a watermarked, reduced data signal; and

adding said watermarked, reduced data signal to said remainder signal to produce an output signal.

2. The method of claim 1 wherein the step of adding said watermarked, reduced data signal to said remainder signal comprises:

embedding a second watermark into said remainder signal to produce a watermarked remainder signal; and

adding said watermarked, reduced data signal to said watermarked remainder signal to produce an output signal.

3. The method of claim 2 wherein at least one of the watermarks is embedded using at least one cryptographic key.

4. The method of claim 2, wherein at least one of the watermarks is embedded using a cryptographic key pair.

5. The method of claim 4, wherein one key of the cryptographic key pair is publicly available while the other key of the cryptographic key pair is secret.

6. The method of claim 1 wherein the data reduction technique comprises a data compression technique.

7. The method of claim 6, wherein the data compression technique comprises a standard lossy protocol for digital signal transmission.

8. The method of claim 6, wherein the data compression technique comprises selective sampling of the data signal in a domain selected from the group comprising the time domain, bit depth domain, and the frequency domain.

9. The method of claim 2, wherein at least one of said first and second watermarks is selected from the group comprising forensic watermarks and universal copy control watermarks.

10. A method of securing a data signal comprising the steps of:

applying a data reduction technique to reduce the data signal into a reduced data signal;

subtracting said reduced data signal from the data signal to produce a remainder signal;

embedding a first watermark into said reduced data signal to produce a watermarked, reduced data signal;

embedding a second watermark into said remainder signal to produce a watermarked remainder signal; and

adding said watermarked, reduced data signal to said watermarked remainder signal to produce an output signal.

11. The method of claim 10 wherein the step of subtracting is comprised of

storing a copy of the data signal; and

subtracting said reduced data signal from the copy of the data signal to produce a remainder signal.

12. The method of claim 10 wherein the data reduction technique comprises a data compression technique.

13. The method of claim 12 wherein the data compression technique comprises a standard lossy protocol for digital signal transmission.

14. The method of claim 12, wherein the data compression technique comprises selective sampling of the data signal in a domain selected from the group comprising the time domain, bit depth domain, and the frequency domain.

15. The method of claim 10, wherein at least one of the watermarks is embedded using at least one cryptographic key.

16. The method of claim 10, wherein at least one of the watermarks is embedded using a cryptographic key pair.

17. The method of claim 15, wherein a copy of said keys is maintained at a central certification authority for reference indemnification purposes.

18. The method of claim 16, wherein one key of the key pair is publicly available while the other key of the key pair is secret.

19. The method of claim 10, further comprising repeating for a finite number of times the steps of

(i) applying a data reduction technique to reduce a previously reduced data signal to produce a further reduced data signal;

(ii) subtracting said further reduced data signal from said previously reduced data signal to produce a further remainder signal; and

(iii) embedding a further watermark into at least one of said further reduced data signal and said further remainder signal;

wherein said adding step to produce an output signal comprises adding all reduced data signals and all remainder signals to produce an output signal.

20. A method of protecting a data signal comprising the steps of:

applying a data reduction technique to reduce the data signal into a reduced data signal;

subtracting said reduced data signal from the data signal to produce a remainder signal;

using a first scrambling technique to scramble said reduced data signal to produce a scrambled, reduced data signal;

using a second scrambling technique to scramble said remainder signal to produce a scrambled remainder signal; and

adding said scrambled, reduced data signal to said scrambled remainder signal to produce an output signal.

21. The method of claim 20 wherein said first and second scrambling techniques are identical.

22. The method of claim 21 wherein the data reduction technique comprises a data compression technique.

23. The method of claim 22 wherein the data compression technique comprises a standard lossy protocol for digital signal transmission.

24. The method of claim 22, wherein the data compression technique comprises selective sampling of the data signal in a domain selected from the group comprising the time domain, bit depth domain, and the frequency domain.

25. A method of securing a data signal comprising:

applying a data reduction technique to reduce the data signal into a reduced data signal;

subtracting said reduced data signal from the data signal to produce a remainder signal;

using a first cryptographic technique to encrypt the reduced data signal to produce an encrypted, reduced data signal;

using a second cryptographic technique to encrypt the remainder signal to produce an encrypted remainder signal; and

adding said encrypted, reduced data signal to said encrypted remainder signal to produce an output signal.

26. The method of claim 25 wherein said first and second cryptographic techniques are identical.

27. The method of claim 25 wherein at least one of said first and second cryptographic techniques is a watermarking technique for embedding at least one digital watermark in a signal.

28. The method of claim 27, wherein at least one watermark is embedded using at least one cryptographic key.

29. The method of claim 27, wherein at least one watermark is embedded using a cryptographic key pair.

30. The method of claim 28 or 29, wherein a copy of said key(s) is maintained at a central certification authority for reference and identification purposes.

31. The method of claim 25 wherein at least one of said first and second cryptographic techniques is a scrambling technique.

32. The method of claim 25 wherein one of said first and second cryptographic techniques is a watermarking technique for embedding a digital watermark in a signal and the other is a scrambling technique.

33. The method of claim 25 wherein said first and second cryptographic techniques are identical.

34. The method of claim 25 wherein the data reduction technique comprises a data compression technique.

35. The method of claim 25 wherein the data compression technique comprises a standard lossy protocol for digital signal transmission.

36. The method of claim 26, wherein the data compression technique comprises selective sampling of the data signal in a domain selected from the group comprising the time domain, bit depth domain, and the frequency domain.

37. A system for securing a data signal comprising:

means to apply a data reduction technique to reduce the data signal into a reduced data signal;

means to subtract said reduced data signal from the data signal to produce a remainder signal;

means to apply a first cryptographic technique to encrypt the reduced data signal to produce an encrypted, reduced data signal;

means to apply a second cryptographic technique to encrypt the remainder signal to

produce an encrypted remainder signal; and

means to add said encrypted, reduced data signal to said encrypted remainder signal to produce an output signal.

38. The system of claim 37 wherein said first and second cryptographic techniques are identical.

39. The system of claim 37 wherein at least one of said means to apply a first and second cryptographic technique utilizes a watermarking technique for embedding a digital watermark in a signal.

40. The system of claim 37 wherein at least one of said means to apply a first and second cryptographic technique utilizes a scrambling technique.

41. The system of claim 37 wherein said means to apply a first cryptographic technique is a means to apply a watermarking technique for embedding a digital watermark in a signal and said means to apply a second cryptographic technique is a means to apply a scrambling technique.

42. The system of claim 37 wherein the data reduction technique comprises a data compression technique.

43. The system of claim 37 wherein the data compression technique comprises a standard lossy protocol for digital signal transmission.

44. The system of claim 37, wherein the data compression technique comprises selective sampling of the data signal in a domain selected from the group comprising the time domain, bit depth domain, and the frequency domain.

45. A system for securing a data signal, said system comprising:

(a) a computer processor;

(b) at least one computer memory;

(c) a data reduction algorithm; and

(d) at least one digital watermarking algorithm;

wherein said computer processor is supplied with programming in conjunction with said computer memory:

(I) to apply said data reduction algorithm to the data signal to yield a reduced data signal, and to subtract said reduced data signal from the data signal to produce a remainder signal;

(II) to embed a first watermark into said reduced data signal by application of said at least one digital watermarking algorithm to produce a watermarked, reduced data signal;

(III) to embed a second watermark into said remainder signal by application of said at least one digital watermarking algorithm to produce a watermarked remainder signal; and

(IV) to add said watermarked, reduced data signal to said watermarked remainder signal to produce an output signal.

46. The system of claim 45, wherein said memory contains a copy of the data signal and said programming to subtract said reduced data signal to produce a remainder signal uses said memory copy of the data signal for the subtraction.

47. The system of claim 42, wherein said at least one digital watermarking algorithm comprises a cryptographic key watermarking algorithm.

48. The system of claim 45, wherein said at least one digital watermarking algorithms comprises two different digital watermarking algorithms.

49. The system of claim 45, wherein said data reduction algorithm comprises a compression algorithm.

50. The system of claim 49, wherein said compression algorithm comprises an algorithm for selective sampling of the data signal in a domain selected from the group comprising the time domain, bit depth domain, and the frequency domain.

51. A method for securing a data signal comprising the steps of:

evaluating the data signal to determine its characteristics and reducibility;

selecting at least one appropriate data reduction technique for the data signal based on the data signal's characteristics;

applying said at least one appropriate data reduction technique to the data signal to produce a reduced data signal;

embedding at least one digital watermark in the reduced data signal; and

supplying an output signal corresponding to the data signal, said output signal comprising said watermark and said reduced data signal.

52. The method of claim 51 wherein the evaluation step comprises:

dividing the data signal into a plurality of discrete data substreams; and

evaluating each of said plurality of discrete data substreams to determine its characteristics and reducibility;

and wherein the selecting step comprises:

selecting at least one appropriate data reduction technique for each of said plurality of discrete data substreams based on the substream's characteristics;

53. The method of claim 51 wherein the appropriateness of said at least one data reduction technique is determined with reference to data signal characteristics selected from

at least one of:

(a) a desired output quality for an output signal;

(b) a desired data reduction ratio;

(c) audio character of data;

(d) video character of data;

(e) text character of data;

(f) executable software character of data.

54. The method of claim 52 wherein the same data reduction technique is used for each of said plurality of data substreams.

55. The method of claim 52 further comprising the steps of performing one of the following techniques upon at least one of said plurality of data substreams:

(a) a scrambling technique;

(b) an encryption technique.

56. The method of claim 55 wherein at least one of said steps of watermarking, scrambling, or encrypting comprises applying at least one cryptographic key.

57. The method of claim 56, further comprising deriving said at least one cryptographic key at least in part from the data signal.

58. The method of claim 56, further comprising deriving said at least one cryptographic key independently of the data signal.

59. The method of claim 51, wherein said step of evaluating the data signal comprises analyzing the data signal with a computer processor implementing an algorithm for analysis of signal characteristics.

60. A method for the protection of a data signal, comprising the steps of:

(a) defining and analyzing a plurality of data substreams within the data signal;

(b) associating at least one key or key pair with data reduction digital watermarking for at least one of said data substreams;

(c) employing said at least one key or key pairs for at least one step selected from the group of:

(i) identifying at least one associated watermark

(ii) encoding at least one associated watermark;

(iii) detecting at least one associated watermark; or

(iv) decoding at least one associated watermark.

61. The method of claim 60, wherein said associated watermarks are selected from the group comprising forensic watermarks and universal copy control watermarks.

62. A method for protected distribution of a data file comprising:

(a) embedding one or more digital watermarks in the data file using data reduction techniques in creating said digital watermark;

(b) and distributing the digitally watermarked file to an end user.

63. The method of claim 62, wherein the use of data reduction techniques comprises creation of a reduced portion of the data file and a remainder portion of the data file.

64. The method of claim 63, wherein the embedding step comprises embedding one or more digital watermarks in each of the reduced portion and the remainder portion of the data file.

65. The method of claim 64, further comprising combining said watermarked, reduced portion with said watermarked, remainder portion to produce the digitally

watermarked file.

66. The method of claim 62, wherein said step of embedding said one or more digital watermarks in the data file is performed on a central computer server and wherein said distributing step is performed by transmitting the digitally watermarked file from the central computer server to an end user output device.

67. The method of claim 66, wherein said step of distributing comprises transmitting the digitally watermarked file over a public data network.

68. The method of claim 66, wherein said step of distributing comprises transmitting the digitally watermarked file over the internet.

69. The method of claim 62, further comprising the step of supplying the end user with means for detecting information about said digital watermark.

70. The method of claim 62, wherein said data file comprises a file selected from the group containing music files, audio files, video files, still image files, streaming media files, and executable computer software files.

71. The method of claim 62, wherein at least one of said digital watermarks created using data reduction comprises a universal copy control watermark for prevention of unauthorized data file copying.

72. The method of claim 62, wherein at least one of said digital watermarks created using data reduction comprises a forensic watermark for tracing at least a portion of the distribution history of the data file.

73. A method for analyzing a data signal that has been embedded with at least one digital watermark using a data reduction technique, said method comprising:

receiving the data signal;

processing the data signal to detect information relative to the digital watermark;

analyzing the detected information to determine if output of the data signal is authorized; and

outputting said data signal if the detected information establishes that output is authorized.

74. The method of claim 73, further comprising the step of precluding output of the data signal if the detected information relative to the digital watermark indicates that output of the data signal is unauthorized.

75. The method of claim 74, wherein said analysis is performed by a consumer electronic device, and further comprising the step of perceptively altering the data signal if the detected information relative to the digital watermark indicates that the output of the data signal is unauthorized.

76. A device for analyzing a data signal that has been embedded with at least one digital watermark using a data reduction technique, said device comprising:

an interface for receiving the data signal;

a detector for processing the data signal to detect information relative to the at least one digital watermark;

an analyzer to analyze the detected information to determine if output of the data signal is authorized or unauthorized; and

an signal generator to output data if the detected information establishes that output is authorized.